

ABSTRACT

[67] Method and system for secure key authentication and key ladder are provided herein. Aspects of the method for secure key authentication may include generating a digital signature of a secure key in order to obtain a digitally signed secure key and transmitting the digitally signed secure key from a first location to a second location. The digital signature may be generated by utilizing an asymmetric encryption algorithm and/or a symmetric encryption algorithm. The digitally signed secure key may be encrypted prior to transmission. The secure key may be a master key, a work key and/or a scrambling key. The digitally signed secure key may be received at the second location and the digitally signed secure key may be decrypted to obtain a decrypted digitally signed secure key.